Lusha's Privacy Practices

White Paper

Version 4.0 - August 2024

Table of Contents:

Please note that the contents of this White Paper are for informational purposes only. Lusha is not qualified to provide legal advice of any kind and is not an authority on the interpretation of any laws, rules, or regulations. To understand how the GDPR, CCPA, marketing laws, or any other laws impact you or your business, you should seek independent advice from qualified legal counsel.

1 Our Privacy Statement

At Lusha, protecting the privacy of our customers and data subjects is of the utmost importance to us: we are committed to data protection and being transparent about our data practices.

We don't just say it; we do it. Lusha's privacy and security practices are audited annually by impartial third parties so that you can rest assured that we, as your data vendor, are compliant and can be trusted. Below is a summary of Lusha's certifications.

Lusha is the only data broker with an **Accredited** ISO 27701 Certification *Privacy Information Management* ISO 27701 Trust Lusha to process personal data in compliance with international standards	Lusha is the only data broker audited and granted with ISO 31700 Certification. *Privacy by Design* Trust that Lusha will not sell its customers' data (also written in the agreement)	Lusha is the only data broker audited and certified by European auditors as *GDPR Compliant* ePrivacyseal Trust Lusha's processes to be compliant with GDPR and German law
Lusha is an IAPP member committed to ensuring that its *legal and compliance team members are IAPP-certified* Trust Lusha's privacy team to handle privacy issues with great care	Lusha is among the few data brokers who have a certified *privacy compliance program* Trust Lusha's industry leading privacy compliance program	Lusha is among the few data brokers that have validated its *CCPA compliance.* Trust Lusha's processes to be compliant with the CCPA/CPRA
SOC2 Type2 Trust that Lusha's internal controls and systems uphold the highest level of information security	ISO 27701 ISO 27701 Trust that Lusha's ISO 27701 certification demonstrates robust privacy and data protection standards	Cloud Security Alliace STAR Level 1 Trust that Lusha's CSA STAR certification demonstrates top-tier security, transparency, and accountability.

2 Professional in-house privacy team

2.1 Lusha's dedicated privacy and compliance team ensures that Lusha remains at the forefront of legislative and regulatory developments. Along with the security, product, engineering, development, and sales teams, they work to ensure the highest standards of privacy protection for its customers and data subjects.

2.2 On 9 March 2021, Lusha announced that all members of its privacy, legal, and compliance team have received certification as privacy professionals from the International Association of Privacy Professionals (IAPP).

2.3 Lusha's privacy and compliance team uses data guidance and first-tier law firms to monitor privacy legislation, regulations, and rulings. It also maintains robust and appropriate policies and practices which will be detailed hereunder.

2.4 Lusha maintains an IAPP corporate membership, which evidences its commitment to giving its team access to the privacy education, resources, and information they need to manage data protection risks and challenges effectively.

2.5 Our Legal and Compliance team:

- Head of Legal and Compliance: Assaf Gilad (CIPP/E, CIPP/US)
- Senior Compliance Manager: Judi Crimmins (CIPP/E)
- Lead Legal Counsel: Diana Berkowitz (CIPP/E)
- Corporate and Commercial Counsel: Caryn Wolfe (CIPP/US)
- Commercial and Procurement Counsel: Hen Kevan

To conclude, Lusha's Privacy, Legal, and Compliance team monitors global privacy regulations and ensures that its research and development practices comply with applicable laws.

3 Privacy landscape and its applicability to Lusha

3.1 Worldwide compliance status

3.1.1 Lusha provides its services worldwide. To comply with ever-changing privacy regulations worldwide, Lusha has obtained ISO 27701 certification, which is the highest international standard for responsibility and transparency in the processing of personal information. Lusha was the first sales intelligence platform to receive ISO 27701 certification and is the only data broker that has earned an accredited ISO 27701 certification which ensures data privacy practices have been thoroughly and independently validated by a recognized accreditation body (Certificate attached hereto as Annex E). This level of scrutiny and credibility is not guaranteed with non-accredited certifications, which may lack rigorous external evaluation. Ultimately, an accredited ISO 27701 certification signifies a commitment to excellence in data privacy management, offering greater protection and peace of mind, and it is also recognized by the CNIL (French data protection authority) as a key factor to evidence GDPR compliance.

3.1.2 Lusha has been certified by ePrivacy (a German state-certified auditor) as GDPR Compliant (and German law compliant). Although Lusha is not subject to GDPR (approved by the CNIL ruling, and by other European data protection authorities via correspondence) as a controller, Lusha voluntarily complies with GDPR and maintains EU and UK representation in the EU (in compliance with Article 27 of the GDPR). In respect to our customers who are subject to the GDPR: Lusha provides all the requirements to act as a processor and comply with the GDPR (Certificate attached hereto as Annex B).

3.1.3 Lusha also validates its compliance with the CCPA by an audit conducted by TrustArc, providing you with the assurance that Lusha's privacy policies and practices meet the Privacy and Data Governance Practices of the California law (Validation Letter attached hereto as Annex D). Lusha is a duly registered data broker in California, Vermont, Oregon, and Texas.

3.1.4 Some of our customers may be subject to the GDPR, CCPA, or other regional privacy laws. Therefore, per request, Lusha can provide all legal documents and evidence necessary to prove its compliance with these and other applicable privacy laws. From time to time, Lusha will publish articles in response to data protection authorities' publications in its Trust Center (e.g., compliance with Dutch regulator guidelines).

For more information, visit our Trust Center.

To conclude, Lusha's processes comply with international standards, EU/UK GDPR and CCPA. To validate this, Lusha undergoes third-party international audits on an annual basis.

3.2 Lusha's role in processing data

3.2.1 Our customers decide independently what personal data to collect and how and why data is processed. Under the GDPR, this would make them data controllers.

3.2.2 When a customer sends Lusha the names and email addresses of their employees, which details are needed to set up accounts with Lusha and provision them as end-users on the customer's account, Lusha acts as a data processor and processes such data solely on our customer's instructions.

3.2.3 By default, during our engagement with our paying customers, any personal data provided to us by our paying customers in our capacity as processor role is not included in our sellable B2B database.

3.2.4 To assure our customers that we do not mix their data with our sellable data, we have created physical separation between the production environment, which keeps our customer data in the EU (within AWS Ireland), and the sellable database, which is maintained on different servers (within AWS Virginia).

3.2.5 To ensure that you can trust us, Lusha has been audited and certified for ISO 31700—Privacy by Design. This is an international standard that outlines requirements and provides guidelines for implementing "Privacy by Design" principles in the design and development of products, services, and systems. "Privacy by Design" is a proactive approach to privacy that integrates privacy considerations into the entire lifecycle of a product or system, starting from its initial design phase and continuing through its development, deployment, and eventual disposal. This provides you with the assurance that Lusha processes the minimum personal data needed to provide its services and does not utilize it for other purposes (Certificate attached hereto as Annex F).

ISO 31700
Privacy by design

3.2.6 Per data sold by Lusha to customers, Lusha will be an independent controller, and the customer will be an independent controller. This is set out in our Data Processing Agreement (DPA).

To conclude, Personal Data provided to Lusha by our customers will be processed in our capacity as a Processor ("Service Provider" under the CCPA). At the same time, Personal Data transferred from Lusha to our customers will be governed by an independent controller-independent controller relationship.

3.3 Data Transfers

3.3.1 Following the Schrems II decision, which invalidated the Privacy Shield program, Lusha withdrew from it and decided to base its international data transfer on the SCCs, as approved by the EU Commission, to establish a lawful transfer of data. These are incorporated by reference in our customer DPA, which is available here.

3.3.2 This DPA contains terms that ensure the confidentiality of your data and incorporates data protection obligations consistent with applicable privacy laws. For a list of third-party subprocessors, including their purpose, locations, and transfer mechanism, see here. Lusha has also signed DPAs and NDAs with all of its subprocessors.

3.3.3 Other than the subprocessors mentioned above, Lusha processes its customer data in Israel (a country with an adequate level of data protection, as decided by this EU Commission adequacy decision) and in the US (by the Lusha US sales and support team). To assist you with the Transfer Impact Assessment, we have prepared this TIA for your reference.

3.3.4 As an additional service offering and for an extra cost, Lusha can exclude the processing of your data in the US. You can ask your sales representative about this service offering; however, please note that in such event, your sales and support representatives will only be available Monday to Friday from 2:00 AM to 5:00 PM (ET), and from 8:00 AM to 5:00 PM (ET) on Sundays.

To conclude, Lushas' customers can trust Lusha to handle their personal data with the highest level of confidentiality and care, not utilize their data for purposes other than providing the services, and process their data in accordance with an adequate level of data protection.

3.4 Legal basis for the processing of business professional contact information

3.4.1 While consent is one basis for lawful processing, it is not the only one. Consent is one of six lawful bases for the processing of data (refer to Article 6(1)(f) of the GDPR). Lusha's legal basis for the processing of personal information is legitimate interest (i.e., providing its services to its customers). Lusha's database is compiled from various sources, including publicly available sources and contributor programs of Lusha and its affiliates (such as the Community Program). All data collected from our data sources are added to Lusha's data lake in which Lusha's proprietary algorithm organizes, scans the data, and merges certain data attributes into a unique identifiable "Business Contact Card," which is located in a highly secure database ("**B2B Database**"). These Business Contact Cards consist of

individuals' professional information that is generally provided on business cards or is often displayed on company websites or in email signatures.

3.4.2 Lusha collects business contact information and other data associated with business professionals to enhance the free market and assist our customers in achieving more business transactions with minimum time and effort.

3.4.3 Since contact data is not collected directly from business professionals, Lusha's processing activities are not based on their consent but on the legitimate interest of both Lusha and its customers, among other legal bases as applicable, depending on the context. The processing operations of Lusha's services are based on two use cases for customers.

3.4.4 Therefore, as explained above, in compliance with Article 14 of the GDPR, Lusha has robust processes in place to inform the data subjects that Lusha holds their personal information. This notice further provides such data subjects with the option to opt out. Sample wording of such notice is available here.

3.4.5 Many advanced privacy regimes provide that personal data must be obtained and processed lawfully and fairly. Personal data should be collected and processed based on a legitimate purpose after balancing the interests of the organization against the interests and rights of the individuals whose data are processed.

3.4.6 With the help of first-tier law firms, Lusha conducted a Data Privacy Impact Assessment ("**DPIA''**) and Legitimate Interest Assessment ("**LIA**") that has led to the conclusion that Lusha's processing of Business Contact Cards satisfies the legitimate interest grounds for processing and is not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

3.4.7 Below is a summary of the findings of the DPIA and LIA. A more expansive summary of our DPIA is available upon request to existing customers or once an NDA is in place.

To conclude, Lusha processes business contact information based on legitimate interest, not consent, in compliance with GDPR, Lusha sends a privacy notice to its contacts in the UK/EEA. A Data Privacy Impact Assessment (DPIA) and Legitimate Interest Assessment (LIA) confirmed that Lusha's processing activities align with legal requirements without infringing on individuals' rights.

4 Lusha's Privacy Practices

4.1 Certifications

Lusha's privacy practices and posture have been independently assessed by multiple third parties. Our attestations include:

4.1.1 **Accredited ISO 27701**: This certification provides a framework for PII holders to establish, implement, maintain, and improve a Privacy Information Management System (PIMS) including compliance with GDPR and other data protection and privacy laws. Lusha has been audited for its data collection, B2B Data enrichment, verification, and prospecting services.

4.1.2 **TRUSTe Enterprise Privacy and Data Governance Attestation**: The TRUSTe Enterprise Privacy Certification aligns with the standards outlined in the TrustArc Privacy and Data Governance Framework, as well as the unique regulatory requirements on which the program is based. The TrustArc framework is based upon globally recognized laws and regulatory standards, such as the OECD Privacy Guidelines, the APEC Privacy Framework, the EU GDPR, and ISO 27001 (Letter of Attestation attached hereto as Annex G).

4.1.3 **TRUSTe CCPA Validation:** Lusha's privacy and data protection practices and governance efforts have been audited against TRUSTe's CCPA Privacy Practices Compliance Validation Requirements and found to meet all the necessary obligations to receive the validation.

4.1.4 **ePrivacyseal EU**: The ePrivacyseal certification attests to a product's compliance with the requirements imposed by EU data protection legislation in accordance with the GDPR. ePrivacy awards the GDPR seal of approval following an in-depth technical and legal audit of a company's digital products.

4.1.5 **ISO 317000:** Concerning Privacy by Design: confirms that Lusha embeds customer privacy considerations in the lifecycle development of its products and services.

4.1.6 **ISO 27001**: Concerning Privacy Security: it confirms that Lusha has been assessed and complies with the requirements of ISO 27001.

4.1.7 **ISO 27018**: Concerning Cloud Security: confirms that Lusha has been assessed and complies with the requirements of ISO 27018 Best Practices.

4.1.8 **SOC 2**: Ensures that Lusha safeguards customer data The standard is based on the following Trust Services Criteria: security, availability, processing integrity, confidentiality, and privacy.

4.2 Accountability

We have taken proactive steps to align our data protection practices with ISO 27701 and GDPR principles and are dedicated to offering the best service to our customers, including by assisting our customers in meeting their obligations under applicable data privacy laws. We take a serious approach to privacy compliance, and set out our main measures below:

4.2.1 Data Accuracy: We are committed to data accuracy. We have implemented an internal mechanism to verify business profile information: each contact within our database must be verified by at least two separate, independent sources to be confirmed as a contact and entered into the database. This substantially mitigates the risk of incorrect or missing information within the database.

4.2.2 Data Minimization: We follow data minimization principles. Our core data set consists of categories of data that are strictly required to provide the services and is limited to basic business profile information (that would typically be found on an email signature or business card).

4.2.3 Fair and Lawful Processing: We ensure that our data processing is fair and lawful, meeting the requirements to lawfully enable the processing. The specific legal bases for processing are set out in our Privacy Policy, but in general, we assess that Lusha's processing of business profile information satisfies the "legitimate interest" basis for lawful processing, with the specific legitimate interest to enable businesses to achieve commercial success through accessing limited professional and business information of individuals (including those in the EU/UK who have not opted out when given the opportunity to do so). To the extent there is a concern that the individual would not reasonably expect further processing, each individual has the right to be removed from our database upon request – see more on individual rights below.

4.2.4 Transparency: We are transparent about the data we process. When we collect business contact information about individuals, where required by law in the EU/UK, we have processes in place to inform the relevant data subjects (by way of notice via email or SMS, as applicable) that Lusha holds their personal information. An example of this notice can be found here. This notice provides the data subject with all relevant information as required by Article 14 of the GDPR, including informing the data subject of their right to opt out and to exercise their other rights as required by law. Further, we have a dedicated privacy center that provides customers and data subjects with relevant and useful information about their data, as well as our privacy and security practices. We strive to provide individuals with

an easy way to exercise their transparency rights, including being able to obtain information about the purposes for which their data is being used and the categories of recipients to whom their data is disclosed (i.e., our customers who license the data for their B2B sales and marketing purposes).

4.2.5 Individual Rights: Individuals, both in our database and customer end-users, can exercise their rights at any time using Lusha's self-service privacy center, where they can exercise control over their personal data profile and are thereby in full control of their data. We honor requests from individuals to opt out of our database, and we maintain a suppression list to ensure the rights are met. We also have processes in place to enable compliance with data subject rights on subject access, rectification, erasure, restriction of processing, and data portability. Lusha honors requests from data subjects to exercise their rights and provides a 24/7 solution to take those requests and comply within 24 hours.

4.3 Security

We implement the following robust security measures:

4.3.1 Encryption: Encrypted data storage solutions so that any personal data processed by Lusha is encrypted whilst in transmission, consistent with industry standards and at a minimum of 256-bit encryption.

4.3.2 Security policies and procedures: Security policies and procedures, including internal security audits, penetration tests, and implementation of security awareness training regarding the handling and securing of personal data to ensure employees and contractors process personal data to a standard aligned with leading data protection laws.

4.3.3 Security standards: To keep personal data safe and secure, such as state-of-the-art encryption (as described above), virus protection, firewalls, and intrusion prevention technologies to prevent any unauthorized access or compromise of Lusha's network, systems, servers, and applications from unauthorized access. Our security standards are audited by third parties and have been certified as meeting the ISO 27701, ISO 27001, ISO 27018 and ISO 31700 standards (as explained above).

4.3.4 Access controls: Access controls to ensure there are limits on access to information systems and facilities to provide reasonable assurance that access to data centers is limited to authorized individuals, such as coded badge access (physical controls), user authentication (logical controls), periodic reviews of changes affecting systems' handling authentication, authorization and auditing as well as privileged

access to production systems and ensuring that any terminated employee's access to personal data will be immediately revoked.

4.3.5 Disaster recovery Involves a formal disaster recovery plan and incident response plans, regular testing of the effectiveness of the plans, and the implementation of backup controls such as periodic backups of production file systems and databases according to a defined schedule and a formal disaster to ensure business continuity and minimize the effects of unplanned events.

4.3.6 Internal policies: Policies and procedures for managing changes to production systems, applications, and databases, including processes for documenting, testing, and approving changes into production, security patching, and authentication.

4.3.7 Confidentiality: Lusha has signed DPAs and NDAs with all service providers. By default, during our engagement with our customers, any personal data that we collect from our subscribed customers in our capacity as processor role is not included in our B2B database unless agreed otherwise.

5 Product features and documentation

5.1 To help our customers comply with the GDPR, we have implemented the following:

5.1.1 Data processing agreement (DPA): We have in place robust data processing agreements with our customers that meet the contractual requirements set forth in Article 28 of the GDPR and can be reviewed here. In respect hereof, we only process personal data provided to us by customers on the instructions of the information-providing customer (as set out in the DPA).

5.1.2 Sub-processor diligence: We undertake thorough due diligence and a security and privacy review of vendors who might process customer personal data. We have procedures in place to ensure that these vendors will not gain access to customer personal data unless they have entered into data processing agreements that meet the Article 28 requirements for compliance with EU/UK laws. Our list of sub-processors, the purpose of processing, the location, and the means of transfer are detailed here.

5.1.3 Data transfers: Personal data is transferred subject to appropriate safeguards. Once we receive your information, we take all appropriate technical and organizational measures and reasonable precautions and follow industry best practices to safeguard your information against loss, theft, unauthorized use, access, or modification. Where applicable, e.g. when our customers are subject to the GDPR and export data to us, we have signed contracts based on the Standard Contractual

Clauses approved by the European Commission or similar contracts, ensuring essentially the same level of protection for further transfers.

5.2 Product Features

5.2.1 Opt-out lists: Data subjects are allowed to exercise their right to opt out of Lusha's data processing. When a data subject opts out of Lusha's database, Lusha notifies customers who have purchased information about the data subject that the data subject has requested be removed. The customer will receive an email stating that the contact has decided to opt out. This email will contain an OTP link that will direct the customer to a landing page. From the landing page, the customer can receive a second email. This email will contain a link to the CSV file containing details of the information that the contact has requested be removed from Lusha's database. Customers are thereafter required to remove such data subject's contact details as acquired using the Lusha Platform unless the customer has an existing relationship with such data subject.

5.2.2 Suppression list: Once a data subject opts out of Lusha's processing of their personal data, Lusha places such information onto a suppression list, thereby avoiding the reappearance of such data subject's personal data on the Lusha Platform in the future.

5.2.3 Hide contacts from specific jurisdictions: This feature allows customers to toggle their account access to any country as desired. For enterprise customers who would like to avoid GDPR and other marketing risks, our platform can be set to hide the information of European individuals (on a country-by-country basis or all of the European Union/European Economic Area).

5.2.4 Admin-control: On a paid subscription, admins have the control to limit the data that their end-users can access from the Lusha Platform.

5.2.5 Do-not-call: Lusha is an official cleaner of the TPS and CTPS in the UK and the DNC in the US. Admin of an account can choose to hide phone numbers listed on these Do Not Call lists.

6 Customer best practices

6.1 Privacy aspects: Customers are independent controllers.

6.1.1 Since Lusha and each of its customers have an independent controller–independent controller relationship with respect to the flow of data from Lusha to the customer, we would like to emphasize that both Lusha and each of our customers have the responsibility to ensure lawful data processing. Other

than for legal and contractually agreed-upon purposes, Lusha will not instruct you how to process your data.

6.1.2 If you enrich your data with Lusha, you already have some legal basis to process the data purchased from Lusha.

6.2 Marketing aspect: Direct marketing practices

6.2.1 Customers must be aware of the legislative and regulatory landscape regarding direct marketing practices in the jurisdiction in which they intend to operate.

6.2.2 Lusha complies with laws applicable to it – but customers have to, too. Each country has its own direct marketing requirements (not to spam, harass, etc.), and certain uses have their own specific requirements as well. Subject to compliance with those laws, our platform can be used for sales, recruiting, marketing, and fraud prevention.

6.2.3 We have created an interactive privacy map to help you determine which laws and legal concepts may apply to your direct marketing approach.

6.2.4 The biggest myth about the GDPR is that consent is the ONLY way to lawfully process personal information on EU data subjects. While consent is one lawful basis for processing, it is not the only one. Most of our customers will process it on a "legitimate interest" basis, which includes direct marketing purposes. (See Id. Art. 6(1)(f), Recital (47).) In that case, consent is not needed, but a transparency notice explaining your processing activities is required (See Id. Art. 14.). So, if you obtain a new list for email marketing, you can include the notice with your first message - however most organizations will send a standalone notice prior to engaging in any commercial activity.

6.2.5 In any case, since emailing a prospect is done only after a sales phone call, most of our customers may not even need for an Art. 14 notice since the conversation over the phone already created a legitimate expectation. Please note that B2B calling is exempted from Do Not Call Lists in many jurisdictions.

7 Additional information we think you should know

7.1 Use of customer data

Lusha requires certain customer information to provide access to the Lusha platform and to set up end-user accounts. Further, if you connect to the CRM, Lusha can provide you with enriched data and relevant insights. Any additional information the customer provides to Lusha is the customer's own choice.

Lusha does not sell customer data; we only share it with subsidiaries and affiliates, service providers, and vendors to provide and improve the service or in connection with an asset sale, merger, bankruptcy, or other business transaction. Further, customer data is kept physically separate, from the contact data that forms Lusha's database.

7.2 Post Termination

Unless the customer breaches our agreement, the Customer may retain the data purchased via Lusha forever.

7.3 AI Usage

Lusha may make certain features available, including artificial intelligence ("**AI**"), machine learning, or similar functionality ("**AI Features**"). These features may include technology developed by Lusha or a third-party provider.

Lusha acknowledges that customer data provided by the customer via its account's integrations and enrich services is confidential. Lusha is committed to safeguarding customer data and respecting its users' privacy. Therefore, Lusha confirms that it will not use customer data to train public AI. Notwithstanding, AI Features may be trained in Lusha's local and offline environment for product and research development purposes, mainly with regard to customers' metadata. For example, AI Features may analyze what certain companies (in the same size and industry as the customer) are searching for in Lusha's Platform and recommend to other customers how to get better enrichment results based on such searches.

Please refer to our Privacy Center for further information.

If you have any questions about our privacy practices, please email us at: privacy@Lusha.com.

Sincerely,

Assaf Gilad (CIPP/US, CIPP/E), DPO

Annex A – GDPR

Lusha: GDPR

At Lusha, privacy is important to us. We are committed to data protection and transparency about our data practices. We have prepared this white paper so you can learn about the data we process, how we use it, and how we comply (and help our customers comply) with relevant privacy laws.

A prevalent data protection law is the EU General Data Protection Regulation or the UK Data Protection Act 2018 (for ease, the "**GDPR**"). The GDPR requires organizations to develop robust data protection programs with an emphasis on accountability, transparency, individual rights, and security. Below, we address the measures Lusha has taken to comply with the GDPR. We do not address each provision of the GDPR but give a broad overview of how the GDPR relates to Lusha and the provision and use of its services.

We are dedicated to offering the best service to our customers, including assisting them in meeting their obligations under applicable data privacy laws. As evidence of our high level of data protection and privacy standards, we have been audited and found to be compliant with ISO 27701 and related GDPR requirements, ISO 27001, ISO 27018, and ISO 31700 (all available on request). Obtaining ISO 27701 is a testament to our unmatched levels of data privacy and compliance in the B2B sales intelligence industry.

1. LUSHA'S ROLE IN DATA PROCESSING AND GDPR COMPLIANCE

1.1. Our customers make independent decisions about what personal data to collect and how and why data is processed. Under the GDPR, our customers would be made independent data controllers. Similarly, we make decisions about the personal data we process, including the information in our database. In this respect, Lusha acts as an independent data controller, and when the data from Lusha's database is transferred to a customer of Lusha, the customer becomes an independent controller of such data. Resulting from the independent controller-independent controller relationship between Lusha and the customer, each party has its own independent obligations under GDPR and other applicable laws. We recommend that customers subject to the GDPR remain cognizant of their own obligations in respect thereto (in addition to potential obligations set out in applicable Marketing Laws (defined below) or otherwise).

1.2. In specific situations, and where a customer is subject to the GDPR, Lusha might be considered a data processor in respect of the processing of data specifically provided by the customer to Lusha. This, for example, occurs when a customer sends Lusha the names and email addresses of their employees, which details are needed to set up accounts with

Lusha and provision them as end-users on the customer's account. In this situation, Lusha acts solely on our customer's instructions.

1.3. Lusha is committed to complying with all laws and regulations to which it is subject, and assisting our customers in meeting their compliance obligations.

2. HOW LUSHA HELPS CUSTOMERS COMPLY WITH THE GDPR

2.1. To help our customers comply with the GDPR, we have implemented the following:

2.1.1. **Data processing agreements (DPAs)**: We have robust data processing agreements in place with our customers that meet the contractual requirements set forth in Article 28 of the GDPR, which can be reviewed here. In respect hereof, we only process personal data provided to us by customers on the instructions of the information-providing customer (as set out in the DPA).

2.1.2. **Sub-processor diligence**: A thorough due diligence and security and privacy review is undertaken in respect of vendors who might process any customer personal data. We have procedures in place to ensure that these vendors will not gain access to customer personal data unless they have entered into data processing agreements that meet the Article 28 requirements for compliance with EU/UK laws.

2.1.3. **Data transfers**: There are certain restrictions on the transfer of data outside of the EU and UK imposed by the GDPR. To ensure the continued protection of the data, any personal data that is transferred is subject to appropriate safeguards. Once we receive customers' information, we take all appropriate technical and organizational measures and reasonable precautions and follow industry best practices to safeguard such information against loss, theft, unauthorized use, access, or modification. Where applicable, e.g., when our customers are subject to the GDPR and export data to us, we have signed contracts based on the Standard Contractual Clauses approved by the European Commission or similar contracts, ensuring essentially the same level of protection for further transfers.

2.2. **Security**: We implement the following robust security measures:

2.2.1. **Encryption**: Encrypted data storage solutions, so that any personal data processed by Lusha is encrypted whilst in transmission, consistent with industry standards and at a minimum of 256-bit encryption.

2.2.2. **Security policies and procedures**: Security policies and procedures, including internal security audits, penetration tests, and implementation of security awareness training regarding the handling and securing of personal data to ensure employees and contractors process personal data to a standard aligned with leading data protection laws.

2.2.3. **Security standards**: Security standards to keep personal data safe and secure, such as state-of-the-art encryption (as described above), virus protection, firewalls, and intrusion prevention technologies to prevent any unauthorized access or compromise of Lusha's network, systems, servers, and applications from unauthorized access. Our security standards are audited by third parties and have been certified as meeting the ISO 27701, ISO 27001, ISO 27018 and ISO 31700 standards (as explained above).

2.2.4. **Access controls**: Access controls to ensure there are limits on access to information systems and facilities in order to provide reasonable assurance that access to data centers is limited to authorized individuals, such as coded badge access (physical controls), user authentication (logical controls), periodic reviews of changes affecting systems' handling authentication, authorization and auditing as well as privileged access to production systems and ensuring that any terminated employee's access to personal data will be immediately revoked.

2.2.5. **Disaster recovery:** Formal disaster recovery and incident response plans, regular testing on the effectiveness thereof, and the implementation of backup controls such as periodic backups of production file systems and databases according to a defined schedule and a formal disaster to ensure business continuity and minimize effects of unplanned events.

2.2.6. **Internal policies**: Policies and procedures for managing changes to production systems, applications, and databases including processes for documenting testing and approval of changes into production, security patching, and authentication.

3. LUSHA'S PRIVACY COMPLIANCE STRATEGY

3.1. We take a serious approach to privacy compliance, and set out our main measures below:

3.1.1. **Accountability**: We take an accountable, privacy-first approach, and in particular, focus on the following:

3.1.1.1. **Data Accuracy**: We are committed to data accuracy. We have implemented an internal mechanism to verify business profile information: each contact within our database must be verified by at least two separate, independent sources to be confirmed as a contact and entered into the database. This substantially mitigates the risk of incorrect or missing information within the database

3.1.1.2. **Data Minimization**: We follow data minimization principles. Our core data set consists of categories of data that are strictly required for the purpose of providing the services and is limited to basic business profile information (that would typically be found on an email signature or business card).

3.1.1.3. **Fair and Lawful Processing**: We ensure that our data processing is fair and lawful, meeting the requirements to lawfully enable the processing. The specific legal bases for processing are set out in our Privacy Policy, but in general, we assess that Lusha's processing of business profile information satisfies the "legitimate interest" basis for lawful processing, with the specific legitimate interest to enable businesses to achieve commercial success through accessing limited professional and business information of individuals [including those in the EU/UK who have not opted out when given the opportunity to do so]. To the extent there is a concern that the individual would not reasonably expect further processing, each individual has the right to be removed from our database upon request – see more on individual rights below.

3.1.2. **Transparency**: We are transparent about the data we process. When we collect business contact information about individuals, where required by law in the EU/UK, we have processes in place to inform the relevant data subjects (by email or SMS, as applicable) that Lusha holds their personal information. This notice provides the data subject with all relevant information as required by Article 14 of the GDPR, including informing the data subject of their right to opt-out. We strive to provide individuals with an easy way to exercise their transparency rights including being able to obtain information about the purposes for which their data is being used, and the categories of recipients to whom their data is disclosed (i.e. our customers who license the data for their B2B sales and marketing purposes). Please refer to our Privacy Policy for further details.

3.1.3. **Individual Rights**: Individuals – both in our database and customer end-users – can exercise their rights at any time. For example, we honor requests from individuals to opt out of our database, and we maintain a suppression list to ensure the rights are met. We also have processes in place to enable compliance with data subject rights on subject access, rectification, erasure, restriction of processing, and data portability. Lusha honors requests from data subjects to exercise their rights (most commonly, the right to be removed from our database).

3.1.4. **Security**: For more information about our security program, see above.

3.2. By default, during our engagement with our customers, any personal data that we collect from our subscribed customers in our capacity as processor role is not included in our B2B database unless agreed otherwise.

3.3. Following the Schrems II decision, Lusha withdrew from the Privacy Shield program and currently only allows for international data transfer based on an executed data processing agreement, which maintains the confidentiality of your data and incorporates data

protection obligations consistent with applicable privacy laws. For a full list of sub-processors visit (and subscribe to updates thereof) our sub-processors page.

4. GDPR APPLICABILITY

4.1. Although we align our data protection practices with the GDPR principles and are determined to be compliant therewith as indicated by our ISO 27701 certification, we do not believe that the GDPR itself applies to us directly regarding the data we provide to our customers for the below reasons:

4.1.1. Lusha is incorporated in the United States, with no 'establishments' in the EU/UK, and therefore does not fall within the territorial scope of the GDPR in respect of the GDPR's establishment criterion.

4.1.2. Lusha does not directly offer its products or services to individuals based in the EU/UK. For example, we do not accept payment for our services in local currency, run local-EU/UK domains for the services or provide the service in an EU/UK language other than English. We only offer our products on a B2B basis, and therefore do not fall within the scope of the GDPR in respect of the offering criterion.

4.1.3. Finally, Lusha does not monitor individuals in the EU/UK, nor does it make decisions or predict preferences and attitudes of such individuals. Lusha does not monitor the contacts in its database within the meaning of the GDPR and therefore does not fall within the territorial scope of the GDPR in respect of the monitoring criterion.

5. USE OF OUR DATA

5.1. We would further like to highlight the different legal roles held by Lusha and each of our customers. While it is incumbent upon Lusha to comply with relevant and applicable privacy laws (such as GDPR), if our customers use the data obtained from Lusha for marketing purposes, they must comply with applicable electronic communication and/or direct marketing laws ("**Marketing Laws**"), which laws are in place to regulate same. The specific Marketing Law(s) with which customers must comply depend on the location of the customer, the location of the data subject receiving the marketing material, and the requirements in respect thereto vary from jurisdiction to jurisdiction. We strongly recommend that customers obtain legal advice on how best to comply with relevant Marketing Laws because the requirements/exemptions for use of data for B2B communications differ.

5.2. If you have any questions about our privacy practices, please email us at: privacy@Lusha.com.

Annex B – GDPR ePrivacy Seal

CERTIFICATE

no. 432/23

ePrivacyseal GmbH
Große Bleichen 21, 20354 Hamburg, Germany

hereby certifies* that

as determined in the certification decision of 20 January 2023

Lusha Systems Inc.
800 Boylston Street, Suite 1410, Boston, MA 02199, United States
as a controller in the sense of art. 4(7) GDPR

operates its product or service
„Prospecting Platform" and "Integrations"
version 10/10/2022
as defined in annex 1 and to the exclusion of the processing activities in annex 2 to this certificate.

final audit day: 20/01/2023
next planned monitoring by 19/01/2026
period of validity: 20/01/2023 – 19/01/2026

Annex C – CCPA/CPRA

Lusha: CCPA/CPRA

This annex summarises our interpretation of the CCPA/CPRA as it applies to Lusha's product and its use thereof by our customers. Data subjects (as defined in the GDPR) are referred to herein as 'consumers.'

Lusha is a registered data broker in the State of California.

Pursuant to Section 999.305(d) of the regulations issued by the California Attorney General in October 2019, a business that does not collect its data directly from the consumer is not required to provide the "pre-collection" notice. However, such businesses are required to notify the consumer directly prior to selling that consumer's information. The notice must state that the business sells information about the consumer and notify the consumer of their right to opt-out.

In order to comply with this requirement, Lusha has provided, and will continue to provide, direct notifications to all California-based contacts in its database. Further, Lusha has an automated process for providing notifications to any new California-based contacts as they are added over time. We have also expanded the notification process to cover our entire database so that we are providing notices regardless of the consumer's location.

In addition to the direct, pre-sale notification requirement, the CCPA requires businesses to disclose certain information to consumers regarding the collection and processing of personal information, as well as describe certain consumer rights, such as the right to opt-out. These disclosures are included in Lusha's privacy notice, available at https://www.lusha.com/legal/privacy_notice/.

Consumer Rights

In addition to the notice and disclosure requirements, the CCPA grants California consumers the right to know what information a business has about them, to opt-out of the sale of information, and to have their information deleted. Lusha maintains a dedicated Privacy Center where individuals may exercise their rights accessible at https://www.lusha.com/privacy-center/. Further, they may select the "Do Not Sell My Info" button on our homepage. From within the Privacy Center, a consumer can submit a request to access the information we have about them or submit a deletion or opt-out request. Consumers can also claim their profile, which allows them to not only view their information but make changes if they wish. Access, opt-out, and deletion requests are handled by our

dedicated privacy team and typically processed within 7 business day, far less than the 45 days allotted under the regulations.

Use of Lusha Data and Other Personal Information

Pursuant to Section 999.305(d), because our customers are obtaining this information from us and are not selling it, they do not need to provide active notifications to the contacts obtained from Lusha. If our customers are subject to the CCPA, however, they will need to honor consumer requests to access and delete their data from your possession, in addition to the other compliance protocols undertaken in respect of the CCPA, such as updating privacy notices.

Annex D – CCPA Validation Letter

Independent CCPA Validation Findings Letter

To the Management of **Lusha Systems, Inc.**

Scope

TRUSTe LLC ("TRUSTe"), an independent subsidiary of TrustArc Inc ("TrustArc") has reviewed the **Privacy Program** of **Lusha Systems, Inc.** ("Organization") as of **April 6, 2024** against 66 CCPA Controls ("Controls"). These Controls are based on the mapping of the California Consumer Privacy Act (CCPA) to the TrustArc Privacy & Data Accountability Governance Framework, The Controls focus on measures for demonstrating that the processing of personal information conducted by **Lusha Systems, Inc.** is performed at a control effectiveness level consistent with CCPA requirements. The Controls cover the following nine areas aligned with the **BUILD**, **IMPLEMENT** and **DEMONSTRATE** Standards set forth in the TrustArc Privacy & Data Governance Accountability Framework, for establishing, maintaining, and continually improving CCPA compliant practices.:

1. **Processes**, including implied requirements for maintaining data inventory about California residents, and developing policies and processes for managing access and individual rights requests.
2. **Awareness and Training,** ensuring individuals responsible for handling individuals rights requests receive training on CCPA requirements for handling such requests.
3. **Use, Retention and Disposal**, including data retention periods, de-identified data, restrictions on selling consumer data, and limited use of information collected for identity verification.
4. **Disclosure to Third Parties and Onward Transfer**, including practices relating to managing service providers such as requiring deletion of consumer personal information, appropriate contracts are in place, and assessments are conducted.
5. **Choice and Consent**, including Do Not Sell Rights and consent to financial incentives.
6. **Access and Individual Rights**, including right to have business provide information regarding consumer's personal data, deletion, data portability and do not sell, and non-discrimination for exercising rights and mechanism to exercise rights.
7. **Transparency**, including privacy notices, clear access to privacy notices and mechanisms to exercise do not sell rights.
8. **Monitoring and Assurance**, including seeking guidance from CA State Attorney General on how to comply with CCPA.
9. **Security,** including employee awareness, risk assessments, safeguards, and incident detection

Organization's Responsibilities

In connection with the Validation, **Lusha Systems, Inc.** was responsible for providing information through a CCPA Validation Assessment regarding its CCPA compliance practices and demonstrating with supporting evidence how it implemented the Controls.

Responsibilities of TRUSTe

Our responsibility was to determine whether **Lusha Systems, Inc.**'s CCPA Privacy Practices within the scope described above comply with the Controls based on the information provided by the Organization. A member of the TrustArc Global Privacy Solutions team reviewed the CCPA Validation Assessment submitted by the Organization and the evidence provided to demonstrate compliance with the Controls upon the Organization having completed remediation of gaps identified by TrustArc's Privacy Intelligence technology. TRUSTe determined whether the provided evidence was sufficient to demonstrate compliance with the Controls and validate that the Organization has met the applicable Controls.

Inherent Limitations

Because of their nature and inherent limitations, practices-level measures of the Organization may not always operate effectively to meet the applicable Controls. Furthermore, our findings herein are subject to the risk that the Privacy Practices, or any component of the Organization's practices, may change or that practice-level measures implemented by the Organization may become ineffective or fail.

Findings

In our opinion, in all material respects, based on the descriptions and supporting evidence of practices-level measures identified in the CCPA Validation Assessment:

- The applicable practices-level measures as further described in the accompanying CCPA Validation Report have been implemented as of **April 6, 2024**.
- The measures described in the CCPA Validation Assessment were suitably designed to provide reasonable assurance that the Controls would be met if the practices-level measures operated effectively as of **April 6, 2024**.

Restricted Use

This Findings Letter and the accompanying report is for the intended use of **Lusha Systems, Inc.** as of **April 6, 2024**:

- This Findings Letter and the accompanying CCPA Validation Report, and any Summary, provided by TRUSTe may be used by the Organization until the expiration date listed below.
- Only the Findings Letter and accompanying CCPA Validation Report represent the official validation determination of TRUSTe.
- Any modifications or alterations to the Findings Letter, the accompanying CCPA Validation Report, or any Summary, from the versions of those documents issued by TRUSTe shall render those documents invalid.
- Organizations must undergo a new CCPA Validation in order to make any representations whatsoever as having been determined as CCPA compliant by TRUSTe,

TrustArc, or any subsidiary or successor in interest to TRUSTe or TrustArc, after the expiration date.

- This Findings Letter can be shared with the Organization's customers, contractors, and other stakeholders until the expiration date.
- This Findings Letter, the accompanying report, and any Summary provided by TRUSTe may be published on the authorized corporate web site(s) of the Organization, as listed in the Annex to this Findings Letter.
- This Findings Letter expires on **April 6, 2025**.

This Findings letter and the accompanying report are not intended to be, and should not be used nor relied upon by anyone other than the Organization and, as determined in the sole discretion of the Organization, the Organization's customers, contractors and other permitted stakeholders.

TRUSTe LLC
April 6, 2024

Annex E – ISO 27701

RONET
International Certification Services Ltd.
Certifies that Privacy Information Security management system of:

Lusha systems Inc

800 Boyton street, suite 1410
Boston, MA
USA

Has been assessed and registereg as meeting the International Standard requirements of:

ISO 27701:2019

Within the scope of activities detailed below:

Privacy information security within development, sales and support of Lusha platform

Within the above stated scope, the role of the organization is:

Processor and Controller

The integrated SoA version for ISO 27001 controls and ISO 27701 controls is 03 December 2023.

Ronen Tuchfeld C.E.O

Effective From: 04 April 2024 Valid Until: 31 October 2025

Original Approval Date: 04 April 2024 Certification No.: P5902

ISO 27001 certificate no. I5902 valid until 31 October 2025
The organization fullfils both ISO 27001 and ISO 27701 controls
*Please see attached an assessment schedule containing site informarion

This certificate remains valid subject to satisfactory Surveillance visits conducted by RONET I.C.S. Ltd.
With accordance to the agreement and code of practice.
Main office: Maor 7, M.P. Hefer 38830, IL
www.ronet-ics.com

ANAB ANSI National Accreditation Board ACCREDITED ISO/IEC 17021-1 MANAGEMENT SYSTEMS CERTIFICATION BODY

RONET International Certification Services Ltd.

Annex F – ISO 31700

RONET
International Certification Services Ltd.
Certifies that Privacy by design for consumer goods and services management system of:

Lusha systems Ltd

132 Menachem Begin st.
Tel Aviv, Israel

Has been assessed and registered as meeting the International Standard requirements of:

ISO 31700-1:2023

Within the scope of activities detailed below:

Privacy by design within development, sales and support of Lusha platform

Ronen Tuchfeld C.E.O

Effective From: 07 July 2024 Valid Until: 31 October 2025

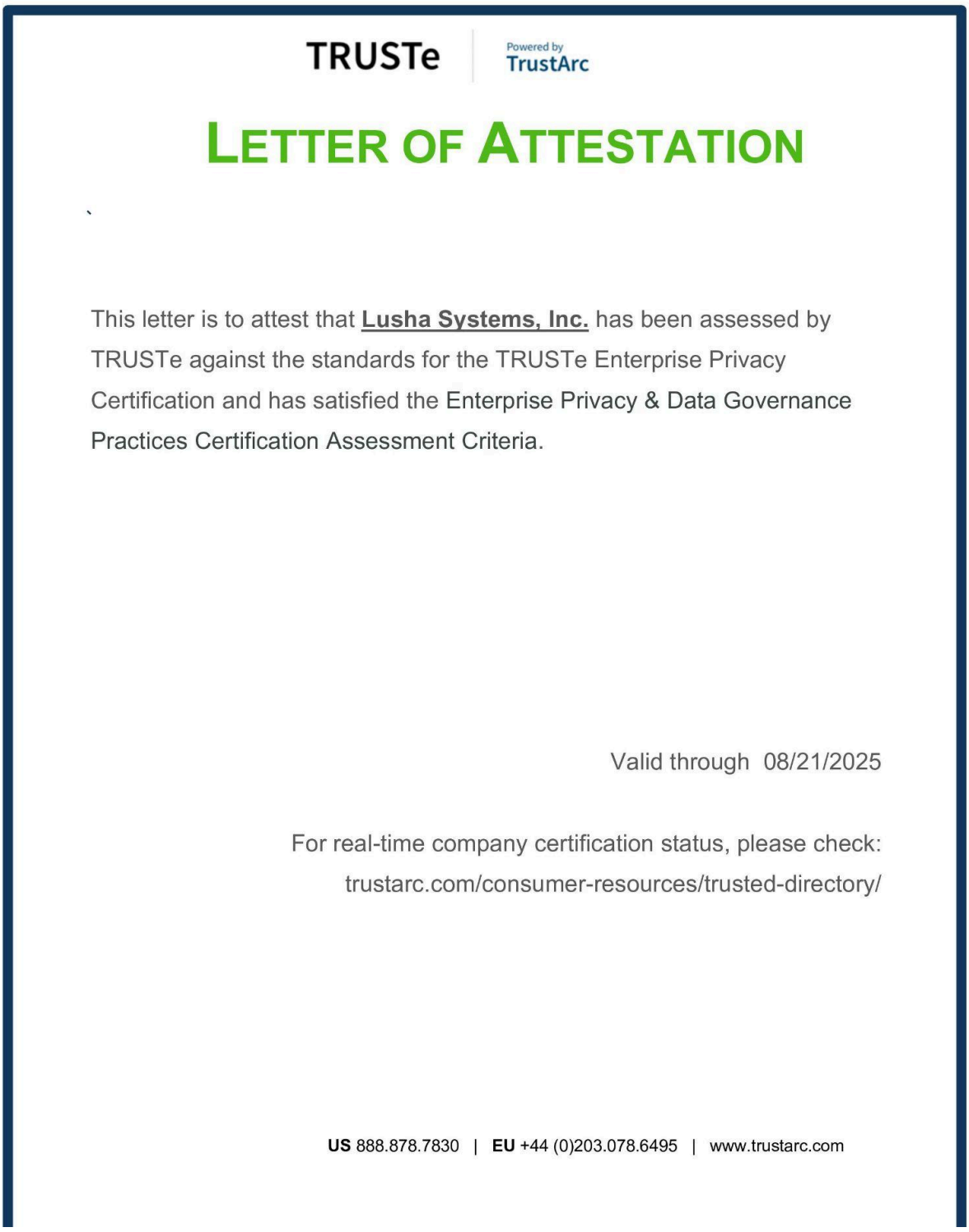
Original Approval Date: 07 July 2024 Certification No.: 5902

ISO 27701 certificate no. P5902 valid until 31 October 2025
The organization fullfils both ISO 27001 and ISO 27701 controls

This certificate remains valid subject to satisfactory
Surveillance visits conducted by RONET I.C.S. Ltd.
With accordance to the agreement and code of practice.
Main office: Maor 7, M.P. Hefer 38830, IL
www.ronet-ics.com

RONET
International Certification Services Ltd.

Annex G – TRUSTe Enterprise Privacy and Data Governance Attestation



TRUSTe | Powered by TrustArc

LETTER OF ATTESTATION

This letter is to attest that **Lusha Systems, Inc.** has been assessed by TRUSTe against the standards for the TRUSTe Enterprise Privacy Certification and has satisfied the Enterprise Privacy & Data Governance Practices Certification Assessment Criteria.

Valid through 08/21/2025

For real-time company certification status, please check:
trustarc.com/consumer-resources/trusted-directory/

US 888.878.7830 | **EU** +44 (0)203.078.6495 | www.trustarc.com